POLICING PEGASUS: THE PROMISE OF U.S. LITIGATION FOR COMMERCIAL SPYWARE ACCOUNTABILITY

Michael Silberman*

A secretive, new weapon is steadily challenging the global balance of power. Authoritarian and democratic regimes alike are clamoring for commercially available "spyware" technologies that enable them to surreptitiously track and monitor the private communications of almost anyone, anywhere in the world.

The leading spyware vendor, NSO Group, has become infamous for its Pegasus product, which has been linked to invasive, high profile digital attacks on journalists, political dissidents, lawyers, and activists around the world. These attacks not only violate human rights but have also led to physical violence and death.

The proliferation of military-grade digital surveillance tools through an unregulated commercial spyware market presents a growing threat to democracy and human rights, from press freedoms to fundamental rights of privacy, expression, assembly, and association. For governments, including the United States, commercial spyware is both a compelling new intelligence tool as well as a significant national security challenge. Major technology platforms are also implicated in the rise of the spyware industry, given the significant resources they must invest in countermeasures to protect their products and users from attacks.

Thus far, international regimes governing both state and non-state actors' commitments to human rights have failed to sufficiently regulate the spyware industry. However, a wave of court cases in the United States represents a novel opportunity to hold spyware firms accountable for human rights violations stemming from the use of their products. After introducing the Pegasus spyware technology and its human rights impacts, this Note reviews the viability of existing international governance and accountability mechanisms—international human rights law, export regimes, industry self-regulation, and multi-stakeholder proposals—in the context of spyware regulation. Finally, this Note examines three cases against NSO in U.S. courts to show how technology firms and individuals may be able to hold NSO liable for illegal activities in the absence of other effective regulatory regimes.

---

* Michael Silberman is an advisor to civil society organizations on emerging technology; Master of Law and Technology, Georgetown Law; B.A., Middlebury College. This work benefited from support and feedback

TABLE OF CONTENTS

INTRODUCTION

The surveillance state George Orwell imagines in his dystopian classic *1984* depicts a helicopter that "skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the police patrol, snooping into people's windows."[1] Indeed, for decades, government surveillance involved agents undertaking significant risks and going to great physical lengths to capture private information—from wiretapping phone lines to hiding audio or video recording devices in a target's personal spaces.

from Anupam Chander as well as the editors of the Georgetown Law Technology Review.

[1] GEORGE ORWELL, 1984, at 4 (1949).

Today, governments need little more than the Internet to remotely break into—or "hack"—a target's device from the safety of an office located anywhere in the world. As the highly publicized hack of Clinton presidential campaign chair John Podesta's email account made clear, a hacker in 2016 needed only to trick a target into providing access to their account or device, such as through phony password reset instructions or other schemes that, once clicked or activated, secretly installs spyware to run in the background.

As cyberattacks naturally evolve and become more sophisticated, a burgeoning cybersecurity industry continues to grow to help individuals, businesses, and governments protect their data from intrusion. In turn, hackers develop novel exploits. But what if there was a way to sidestep this cat-and-mouse game by breaking in through the "back door" instead of the front, leaving no trace? That's exactly what the NSO Group achieved through its groundbreaking Pegasus technology. Pegasus has been described as a type of magic because of its unique ability to access the entirety of a target's phone (and, therefore, intimate details of one's entire life) using nothing more than a telephone number. The target of a Pegasus attack does not need to be tricked, make a mistake, or engage with anything at all; in industry terms, it is a "zero-click" attack. The target can also be anywhere in the world, which means a government agent can access a political exile's entire network without ever crossing borders.

But Pegasus and its creators, the NSO Group, did not make headlines simply because the tool represents a technological breakthrough. NSO Group is under intense global scrutiny because it has democratized espionage and enabled some of the most repressive and authoritarian governments in the world to spy on opponents or journalists in ways that were previously inaccessible or unaffordable. "In countries with few resources, security forces can now pursue high-tech operations using off-the-shelf technology that is almost as easy to acquire as headphones from Amazon," observes Ron Deibert, a leading spyware researcher.[2]

In July 2021, the Pegasus Project, a consortium of sixteen global media outlets coordinated by Forbidden Stories, revealed that Pegasus was not just being used by its clients to surveil shortlists of suspected terrorists or criminals, as promised by NSO Group. The investigation showed that Pegasus had been used widely against more than 50,000 members of civil society, including human rights

[2] Ronald J. Deibert, *The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy*, FOREIGN AFFAIRS (Dec. 12, 2022), https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert [https://perma.cc/MY27-RTGM].

activists, journalists, academics, religious figures, and lawyers.[3] Among those targeted with Pegasus were the wife, fiancée, and relatives of the murdered Saudi journalist and critic, Jamal Khashoggi, before and after his brutal murder in 2018 by Saudi operatives.[4] NSO Group has repeatedly denied that its products were used to target Khashoggi, his associates, or his confidants.[5]

The proliferation of commercial spyware like Pegasus is not only a threat to human rights: it is also a national security issue. In 2020 and 2021, devices belonging to officials at the United Kingdom's (U.K.) Foreign Commonwealth and Development Office were hacked with Pegasus along with a device located at the Prime Minister's residence, 10 Downing Street.[6] In March 2023, the White House said that at least fifty U.S. government employees had been suspected or confirmed to have been targeted with commercial spyware.[7] At the same time, President Biden announced a government-wide ban on the use of commercial spyware due to national security concerns, calling out Pegasus by name.[8]

Since NSO Group does not itself target individuals through Pegasus software but instead provides states with the means to do so, what responsibility does the company bear for the actions of its clients—especially if states choose to use the product in ways unintended by the provider? Even NSO Group acknowledges the potential dangers, writing in one of their reports that they "are fully aware that if a customer misuses one of [their] products it could lead to the harm of the human rights of an individual not involved in

---

[3] *See* Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani & Michael Safi, *Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon*, THE GUARDIAN (July 18, 2021), https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus [https://perma.cc/YV4T-8XQ9] [hereinafter Pegasus Project].

[4] *See* Lesley Stahl, *CEO of Israeli Spyware-maker NSO on Fighting Terror, Khashoggi Murder, and Saudi Arabia*, CBS (May 14, 2019), https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/ [https://perma.cc/SJ8W-DQMK].

[5] *See id.*

[6] *See* Deibert, *supra* note 2.

[7] *See* Kevin Collier, *At Least 50 U.S. Government Employees Hit with Spyware, White House Says*, NBC (Mar. 27, 2023), https://www.nbcnews.com/tech/security/least-50-us-government-employees-hit-spyware-white-house-says-rcna76820 [https://perma.cc/KNK4-PX8P].

[8] *See id.*

serious crime or terrorism, particularly to such individual's rights to enjoy privacy or freedom of opinion and expression."[9]

By some estimates, more than 500 companies develop, market, and sell surveillance tools to governments.[10] Therefore, the question of how to regulate this growing industry extends beyond NSO Group. The former U.N. Special Rapporteur on freedom of opinion and expression, David Kaye, is one of many who warns that the current regulatory regime for commercial spyware is wholly insufficient: "The private surveillance industry is a free-for-all . . . an environment in which States and industry are collaborating in the spread of technology that is causing immediate and regular harm to individuals and organizations that are essential to democratic life – journalists, activists, opposition figures, lawyers, and others."[11]

Some of the commercial spyware industry's threats to democracy and individual rights are covered by international law, which outlines human rights obligations for states as well as firms. Under the International Covenant on Civil and Political Rights (ICCPR), governments must not unlawfully or arbitrarily intrude upon individual freedoms of privacy, expression, assembly, and association.[12] The United Nations Guiding Principles on Business

---

[9] NSO GROUP, HUMAN RIGHTS POLICY 1 (2019).

[10] *See* Rep. of the Off. of the U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, ¶ 6, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022) [hereinafter UNHCR].

[11] Press Release, U.N. Off. of the High Comm'r for Hum. Rts., UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools (June 25, 2019), https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance [https://perma.cc/7NHN-72HW].

[12] *See* International Covenant on Civil and Political Rights, Dec.19, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]. Article 17 covers rights to privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." *Id.* art. 17. Article 19 protects freedoms of expression: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." *Id.* art. 19. Article 21 protects "the right of peaceful assembly." Article 22 protects freedoms of association: "Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests." *Id.* art. 21. Although the text varies slightly by Article, the ICCPR generally stipulates that restrictions on these rights must be proscribed by law and "necessary in a democratic society in the interests of national security or public safety, public order (ordre public),

and Human Rights (UNGPs) compel firms like NSO Group to conduct due diligence and "avoid causing or contributing to adverse human rights impacts."[13] Nevertheless, NSO Group has furnished Pegasus to numerous governments with abysmal human rights records, including Saudi Arabia, which reportedly used Pegasus to facilitate the Khashoggi murder.[14]

The U.S. is becoming a key battleground for legal challenges against NSO Group. In 2019, WhatsApp and its parent company, Facebook (now Meta), filed a complaint in U.S. federal court alleging that NSO Group violated the Computer Fraud and Abuse Act (CFAA) and a related state statute, violated contracts (terms of service), and trespassed its servers.[15] NSO Group, an Israeli company and Israeli government contractor, has unsuccessfully appealed all the way to the Supreme Court, claiming foreign official immunity and derivative sovereign immunity in an attempt to have the case dismissed. In late 2021, Apple filed its own complaint in federal court, making similar claims against NSO Group for targeting Apple's software and its customers, Apple users in the United States.[16] A year later, fifteen journalists affiliated with the Salvadorian publication *El Faro* became the first individuals to file a federal complaint against NSO Group for hacking their mobile devices.[17]

This Note proceeds as follows. First, I highlight what makes Pegasus and the new commercial spyware industry unique from prior generations of cyber-surveillance. Next, I review the limits of

---

the protection of public health or morals or the protection of the rights and freedoms of others." *Id.* art. 21.

[13] U.N. Off. of the High Comm'r for Hum. Rts, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework*, ¶ 13, U.N. Doc. [ST/]HR/PUB/11/4 (2011) [hereinafter UNGP].

[14] *See* Corin Faife, *New Analysis Further Links Pegasus Spyware to Jamal Khashoggi Murder*, THE VERGE (Dec. 21, 2021), https://www.theverge.com/2021/12/21/22848485/pegasus-spyware-jamal-khashoggi-murder-nso-hanan-elatr-new-analysis [https://perma.cc/R9G8-4HJH].

[15] *See* Complaint & Demand for Jury Trial, WhatsApp v. NSO Grp. Techs. Ltd., No. 19-07123 (N.D. Cal. Oct 29, 2019) [hereinafter WhatsApp Complaint].

[16] *See* Complaint & Demand for Jury Trial, Apple Inc. v. NSO Grp. Techs. Ltd., No. 21-09078 (N.D. Cal. Nov. 23, 2021) [hereinafter Apple Complaint].

[17] *See* Complaint & Demand for Jury Trial, Dada v. NSO Grp. Techs. Ltd., No. 22-07513 (N.D. Cal. Nov. 30, 2022) [hereinafter Dada Complaint].

existing and proposed international legal mechanisms to influence NSO Group's operations; specifically, international human rights law, export control law, industry self-regulation, and multi-stakeholder approaches. Finally, I examine the three pending legal claims against NSO Group in U.S. courts to demonstrate the potential power of technology firms as well as individual victims to hold NSO Group liable for its actions under U.S. law. In the absence of effective global governance or accountability regimes for the commercial spyware industry, the outcome of these cases has the potential to impact NSO Group's operations as well as that of other commercial spyware firms located outside of the United States.

I. HUMAN RIGHTS IMPLICATIONS OF A GROWING COMMERCIAL SPYWARE INDUSTRY

State-sponsored surveillance tactics have long been designed and developed by state intelligence units—until recently. Today, a rapidly growing private industry is enabling governments of all stripes to access surveillance technologies they could not have previously afforded or been able to develop on their own. Given the significant engineering resources required to develop sophisticated digital surveillance tools that can outsmart and outpace engineering and security teams at the world's largest and arguably most innovative technology firms, like Google, Apple, Microsoft, digital surveillance has naturally been limited to countries like China and the United States that can afford massive investments in cyber espionage. Even the U.S. government, with one of the world's largest counterterrorism and law enforcement budgets, was unable to break into the iPhone of the suspected San Bernadino mass shooter using the agency's own toolset in 2015.[18]

Commercial spyware changes the game. Spyware vendors such as NSO Group, not to mention their government clients, defend the use of this invasive technology as essential to protecting citizens from crime and terrorism. NSO Group claims that it licenses its products only to law enforcement and intelligence agencies of sovereign states, and that its surveillance tool "must only be directed

[18] *See* Mitchell Clark, *Here's How the FBI Managed to Get into the San Bernardino Shooter's iPhone*, THE VERGE (Apr. 14, 2021), https://www.theverge.com/2021/4/14/22383957/fbi-san-bernadino-iphone-hack-shooting-investigation [https://perma.cc/S9EY-MEXZ]. The FBI relied on a private Australian firm to hack the device because the agency was unable to access the locked iPhone using its own resources. *See id.*

by [its] operators at legitimate criminal or terror group targets."[19] At the same time, states' use of spyware technology has invaded individuals' privacy and has led to serious human rights violations ranging from arbitrary detention and torture to death.[20] NSO Group admits that its tools have been misused and acknowledges the "inherent human rights tensions associated with [its] products."[21]

Part I.A situates Pegasus in the context of a growing global spyware industry. Part I.B summarizes the spyware's unique ability to invade an individual's privacy. Finally, Part I.C shows how the technology's use can lead to significant human rights abuses.

A. A Growing Commercial Spyware Industry

Estimated to be worth twelve billion dollars, the commercial spyware industry is big business.[22] NSO Group is arguably the most prominent vendor and has been valued at more than one billion dollars.[23] In its court filings, Apple shows that NSO Group's products and services generate hundreds of millions of dollars in revenue and that the company charges tens of millions of dollars per customer for its products and services, sometimes charging over one hundred million dollars for a single license.[24] "The big, dirty secret is that governments are buying this stuff—not just authoritarian governments but all types of governments," said a Microsoft executive who leads the company's fight against spyware.[25] Indeed, over the past decade, at least seventy-four governments contracted with commercial firms to acquire spyware or digital forensics technology.[26]

While some of the most publicized abuses of commercial spyware are associated with authoritarian regimes like Saudi Arabia and the United Arab Emirates (UAE) using spyware against political

---

[19] NSO GROUP, TRANSPARENCY AND RESPONSIBILITY REPORT 2 (2021) [hereinafter TRANSPARENCY AND RESPONSIBILITY]

[20] UNHCR, *supra* note 10, ¶ 9.

[21] TRANSPARENCY AND RESPONSIBILITY, *supra* note 19, at 9.

[22] *See* Ronan Farrow, *How Democracies Spy on Their Citizens*, NEW YORKER (Apr. 25, 2022), https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

[23] *See id.*

[24] Apple Complaint, *supra* note 16, ¶ 55.

[25] Farrow, *supra* note 22.

[26] STEVEN FELDSTEIN & BRIAN KOT, WHY DOES THE GLOBAL SPYWARE INDUSTRY CONTINUE TO THRIVE? TRENDS, EXPLANATIONS, AND RESPONSES 1, 9 (Carnegie Endowment for Int'l Peace ed., 2023).

opponents and dissidents, democracies like the United States have been equally invested in adopting spyware over the past decade in the name of counterterrorism and crime prevention.[27] In the last year, state agencies in four European countries—Greece, Hungary, Poland, and Spain—have been accused of deploying spyware against journalists and political opposition figures.[28]

The rise of digitally enabled protest movements like the Arab Spring and color revolutions has also contributed to the growth of the spyware market. "By offering an almost godlike way to get inside activist networks," argues Ron Deibert, "spyware has opened up a powerful new method for governments to monitor dissent and take steps to neutralize it before large protests occur."[29] Even if they can't prevent a popular uprising, threatened political leaders and governments can now turn to spyware in an effort to prevent the next uprising.

B. How Pegasus Remotely Infiltrates a Targeted Individual's Device

Pegasus is neither the first nor the only commercial spyware product; yet, it has become infamous for its novel ability to be remotely installed on a target's device without the owner's awareness or consent. While other spyware infections typically require a target to click on a link or open a file (i.e. "phishing"), Pegasus' "zero-click" exploits infect Android and iOS devices through vulnerabilities in WhatsApp's messaging app and Apple's iMessage software.[30] Once a device is infected with Pegasus, operators can not only remove any visible traces of an attack but also remotely access the device owner's complete activities, communications (included encrypted messages on Signal and Telegram), and stored data.

A Google analyst described Pegasus' "zero-click" exploit as "one of the most technically sophisticated exploits we've ever seen," noting that Pegasus' capabilities were previously thought to be accessible only to very few states. [31] Now, the technology is available to any government that can pay. Here is how the Pegasus

---

[27] *See* Deibert, *supra* note 2.

[28] *See id.*

[29] *Id.*

[30] *See* BILL MARCZAK, JOHN SCOTT-RAILTON, BAHR ABDUL RAZZAK, NOURA AL-JIZAWI, SIENA ANSTIS, KRISTIN BERDAN & RON DEIBERT, FORCEDENTRY: NSO GROUP IMESSAGE ZERO-CLICK EXPLOIT CAPTURED IN THE WILD 3 (2021).

[31] Deibert, *supra* note 2.

exploit works, according to Citizen Lab, a digital forensics team based at the University of Toronto:

> Once Pegasus is installed, it begins contacting the operator's command and control (C&C) servers to receive and execute operators' commands, and send back the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps. The operator can even turn on the phone's camera and microphone to capture activity in the phone's vicinity, and use the GPS function to track a target's location and movements.[32]

After the discovery of Pegasus exploits in May 2019, WhatsApp and Apple moved quickly to release security patches and software updates that rendered them useless. However, NSO Group perpetuates a cat-and-mouse game to ensure its spyware is still usable by clients. The company regularly develops new exploits—sometimes in a matter of weeks.[33] Therefore, researchers can never know for certain the various ways Pegasus might infect devices. Pegasus is designed to be invisible to anti-virus software, evade forensic analysis, be remotely deactivated and removed by its operators.[34] The following illustration summarizes the ways Pegasus can infiltrate a device and its powerful capabilities once installed:

[32] *NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases*, CITIZEN LAB (Oct. 29, 2019), https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/ [https://perma.cc/JAT7-DNTA].

[33] *See* Farrow, *supra* note 22.

[34] *NSO Group / Q Cyber Technologies*, *supra* note 32.

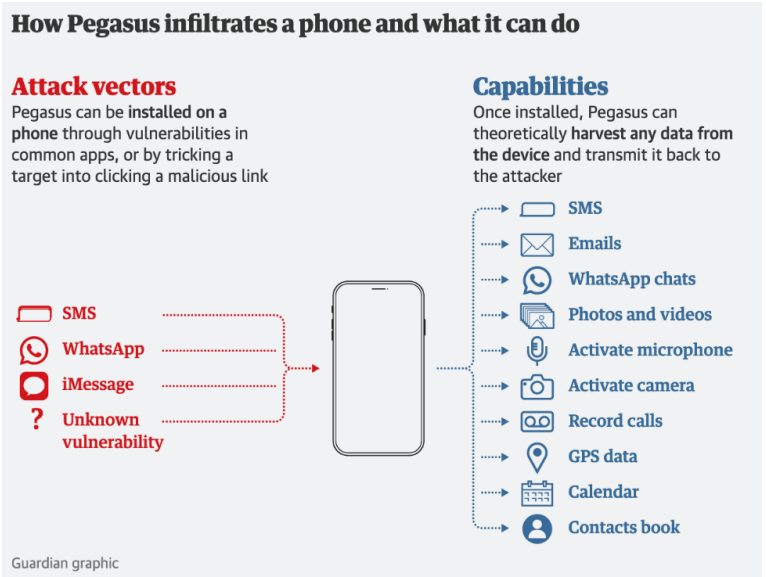

Figure 1*: How Pegasus works* (Source: The Guardian[35])

C. Pegasus Has Been Weaponized Against Civil Society

As early as 2017, the New York Times revealed that Mexico had purchased Pegasus spyware and used it to target prominent human rights lawyers, journalists, anti-corruption activists, and other critics.[36] The government had purchased the product on the condition that the software only be used to investigate criminals and terrorists, per NSO Group's standard terms.[37] A year earlier, Ahmed Mansoor, an award-winning human rights defender imprisoned in the UAE, was also targeted with NSO Group's spyware.[38]

---

[35] David Pegg, Paul Lewis, Michael Safi & Nina Lakhani, *FT Editor Among 180 Journalists Identified by Clients of Spyware Firm*, THE GUARDIAN (July 20, 2021), https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware [https://perma.cc/9D6Y-NJ28].

[36] Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. TIMES (June 19, 2017), https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html [https://perma.cc/9TTJ-WGD3].

[37] *See id.*

[38] BILL MARCZAK, JOHN SCOTT-RAILTON, SARAH MCKUNE, BAHR ABDUL RAZZAK & RON DEIBERT, HIDE AND SEEK: TRACKING NSO GROUP'S PEGASUS SPYWARE TO OPERATIONS IN 45 COUNTRIES 8 (Citizen Lab, Research Report No. 113 2018).

However, widespread government use of Pegasus to spy on journalists, human rights defenders, lawyers, political opposition groups, and other civil society members only became clear the following year. In 2018, Citizen Lab found evidence of operators in forty-five countries using Pegasus spyware to surveil over 50,000 individuals worldwide.[39] In late 2019, Citizen Lab reported over one hundred additional cases of Pegasus being used to target journalists and human rights defenders in at least twenty countries. This report was the result of the team's analysis of a wave of attacks made through the WhatsApp platform earlier that year.[40]

Amid mounting evidence of how Pegasus has been linked to human rights violations, Apple's court filing cites NSO Group's own Transparency and Responsibility Report[41] to show that even "NSO admits that its destructive products have led to violations of 'fundamental human rights,' which have been widely recognized and condemned by human rights groups and governments, including the U.S."[42]

Digital surveillance through spyware has real world implications. As leading human rights NGO Human Rights Watch explains, "information obtained through arbitrary surveillance can be used to prosecute or detain human rights defenders or dissidents, and to monitor and harass those who might dare to stand in the way of government officials or powerful figures."[43] The effects of digital surveillance extend well beyond the targeted individuals and create a "chilling effect on advocates, journalists, and other members of civil society who may self-censor out of fear" of being targeted themselves—including particularly vulnerable victims of abuse and confidential sources.[44] For the nearly 200 journalists who have already been targeted by NSO Group's clients, the risks extend beyond personal harm and signify a broader threat to press freedoms.[45]

Victims of spyware attacks can suffer significant mental anguish and physical harm. Deibert cites the experience of a Saudi activist who explained that "being digitally targeted was a form of

---

[39] *See id.* at 8–9.

[40] *See NSO Group / Q Cyber Technologies*, *supra* note 32.

[41] *See* TRANSPARENCY & RESPONSIBILITY, *supra* note 19.

[42] Apple Complaint, *supra* note 16, ¶ 12.

[43] *Unchecked Spyware Industry Enables Abuses*, HUMAN RIGHTS WATCH (July 30, 2021), https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses **[**https://perma.cc/ZU6X-YY6U] [hereinafter *Unchecked Spyware Industry*].

[44] *Id.*

[45] Pegg et al., *supra* note 35; *see also* UNHCR, *supra* note 10.

'psychological and emotional war' that caused her 'endless fear and anxiety.'"[46] Data analysis spearheaded by Forensic Architecture, a group affiliated with the University of London, suggests that Pegasus attacks may also be linked to physical harm.[47] By plotting known Pegasus infections against reported "physical events," from intimidation to assault to murder, the research team discovered that "[c]yber-surveillance is consistently entangled with a spectrum of physical violations, including break-ins, intimidation, assaults, arrests, lawsuits and smear campaigns, and murder, in the case of prominent Saudi journalist Jamal Khashoggi, whose friends and colleagues were targeted by Pegasus."[48]

The Forensic Architecture team developed an interactive, open-source dataset that surfaces two additionally disturbing patterns from a human rights perspective.[49] First, Pegasus attacks tend to target networks of civil society collaborators: attacks start with one individual and then expand to target the individual's entire professional network.[50] In the examples surfaced by the project, the use of Pegasus occurred during or shortly after "these civil society networks expose or confront controversial or criminal state policy."[51] Second, since digital targeting can easily cross borders, the research shows examples of states targeting dissenters in exile "while also physically targeting their colleagues and families in their home country."[52] One example shows the close proximity between Saudi Arabian dissident video blogger (and Jamal Khashoggi's friend) Omar Abdulaziz being targeted with Pegasus while in exile in Montreal and the arrest of two of his brothers in Saudi Arabia.[53]

In sum, despite the myriad threats posed to individual safety as well as democratic norms through states' abuse of intrusive hacking technologies like Pegasus, demand for these powerful tools continues to grow.

---

[46] Deibert, *supra* note 2.

[47] *How the NSO Group Enables State Terror*, FORENSIC ARCHITECTURE, https://forensic-architecture.org/investigation/digital-violence-how-the-nso-group-enables-state-terror/ [https://perma.cc/78E4-V7U3].

[48] *Id.*

[49] *See id.*

[50] *See id.*

[51] *Id.*

[52] *Id.*

[53] *See id.*

II. LIMITATIONS OF COMMERCIAL SPYWARE ACCOUNTABILITY THROUGH INTERNATIONAL LAW AND GLOBAL GOVERNANCE

The commercial spyware industry is largely unregulated; firms like NSO Group operate with near impunity. International humanitarian laws and regulations, like those governing the use of indiscriminate weapons, do not explicitly exist for commercial spyware. Even NSO Group's former CEO Shalev Hulio acknowledges the gap: "[t]here is the Geneva Conventions for the use of a weapon. I truly believe that there should be a convention of countries that should agree between themselves on the proper use of such tools."[54] A range of international accountability mechanisms, as discussed in this Part, have the potential to limit the proliferation and misuse of commercial spyware: (a) international human rights law, (b) blacklists and export controls, (c) industry self-regulation, or soft law, and (d) proposed multi-stakeholder alternatives. This Part examines the limitations of each of these mechanisms in effectively regulating the commercial spyware market in a human-rights compliant manner.

A. International Human Rights Law Is Unable to Compel State Compliance

The International Covenant on Civil and Political Rights (ICCPR), alongside the United Nations Declaration of Human Rights (UDHR),[55] establishes a universal right to privacy that, if enforced, protects individuals against a state's illegitimate use of spyware. [56] Article 17 of the ICCPR prohibits "arbitrary or unlawful interference with [one's] privacy, family, home or correspondence" and "unlawful attacks on [one's] honour and reputation", and it guarantees everyone legal protection against interferences or attacks on these rights.[57] The ICCPR similarly establishes an individual's rights to freedoms of expression,[58] association,[59] and assembly.[60] Applying the ICCPR, a state can only interfere with an individual's

---

[54] Farrow, *supra* note 22.

[55] *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948). Article 12 of the UDHR states: "No one shall be subjected to arbitrary interference with his privacy, family home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.* at 4.

[56] *See* ICCPR, *supra* note 12.

[57] *Id.* art. 17.

[58] *See id.* art. 19.

[59] *Id.* art. 22.

[60] *Id.* art. 21.

civil rights under specific conditions. According to Asaf Lubin's analysis of decades of jurisprudence, treaties, soft law, and commentary on the use of surveillance technologies by governments, these narrowing conditions can be summed up in the following five principles: legality, necessity, proportionality, adequate safeguards, and access to remedy.[61]

The ICCPR does not prohibit states from using spyware; it simply restricts the circumstances under which the technology can be used—i.e., in furtherance of national security objectives or to protect the rights of others. Of course, these justifications often provide states with broad surveillance authorities under domestic law which may not be legitimate under international law. The United Nations High Commissioner for Human Rights (UNHCR) notes that "hacking by various State actors often seems to pursue goals that are not legitimate under international human rights law."[62] The UNHCR goes on to say that "hacking can never be justified for political or business reasons, which is often the case when human rights defenders or journalists are targeted."[63]

International law only functions when states apply and enforce treaties and customs. With 173 states as parties to the ICCPR, full compliance could go a long way to slow or stop the misuse of spyware. Other political and economic strategies, like sanctions or aid, could be used to pressure any of the remaining eighteen non-signatories, such as Saudi Arabia or South Sudan, into compliance.

However, in his 2019 report to the United Nations, Special Rapporteur David Kaye is less hopeful, describing a near total failure of international human rights law to regulate the use of targeted surveillance technologies: "While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without fear of legal consequence. The human rights law framework is in place, but a framework to enforce

---

[61] *See* Asaf Lubin, *Selling Surveillance* (manuscript at 13) http://ssrn.com/abstract=4323985 **[**https://perma.cc/2744-YCJ7] ("This international human rights framework establishes that intrusions on the rights to privacy and freedom of expression through the use of surveillance tools is only permissible when such measures are prescribed by law that is foreseeable and accessible (principle of legality), where the measure is necessary to achieve a legitimate aim (principle of necessity), where less intrusive means of achieving that aims have been exhausted (principle of proportionality), where ex ante independent authorization and ex post effective review are implemented (principle of adequate safeguards), and where victims of abuse are provided sufficient recourse to judicial remedy (principle of access to remedy)."). *Id.*

[62] UNHCR, *supra* note 10, ¶ 18.

[63] *Id.*

limitations is not."[64] Thus, in 2021, following the revelations on the widespread use of Pegasus against journalists and civil society, the UNHCR Michelle Bachelet found herself in the position of needing to reassert states' obligations under international law: "I would like to remind all States that surveillance measures can only be justified in narrowly defined circumstances, with a legitimate goal. And they must be both necessary and proportionate to that goal."[65]

One possible reason for states' lack of compliance with international law in the context of spyware is ambiguity regarding the right to privacy. Lubin notes that international law around privacy has developed and evolved since the Universal Declaration of Human Rights was adopted in 1948, but "the exact scope of the custom, and the obligations derived from it, is what is often in dispute."[66] Evolving common law around the right to privacy, which varies by region and country, raises questions about whether practices like mass surveillance or facial recognition by law enforcement constitutes a violation of customary international human rights law.[67]

Another potential reason for state noncompliance is the general inadequacy of domestic laws governing the use of new technologies—a common public policy problem extending well beyond the issue of spyware.[68] According to the UNHCR, many states have failed to implement legal guardrails and lack clear, precise, publicly available laws to govern hacking.[69] Even though some states have implemented legal frameworks that comply with international human rights law, others rely on broad rules or outdated laws enacted before the digital age.[70]

---

[64] Off. of the U.N. High Comm'r for Hum. Rts., Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Surveillance and Human Rights*, ¶ 46, U.N. Doc. A/HRC/41/35 (May 28, 2019) [hereinafter Special Rapporteur].

[65] Press Release, Off. of the U.N. High Comm'r for Hum. Rts., Use of Spyware to Surveil Journalists and Human Rights Defenders, Statement by UN High Commissioner for Human Rights Michelle Bachelet, (July 19, 2021), https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner [https://perma.cc/4GWR-AGQD] [hereinafter Bachelet Statement].

[66] Lubin, *supra* note 61, at 14.

[67] *Id.*

[68] Consider, for example, contemporary policy challenges associated with regulating artificial intelligence or moderating content on social media platforms.

[69] *See* UNHCR, *supra* note 10, at 5.

[70] *See id.* ¶ 17.

Lubin also observes an underenforcement problem when it comes to human rights law and spyware: "Due to the secrecy surrounding the practice and the plausible deniability attached to such secrecy, a process of norm internalization is hard to achieve in the context of espionage regulation."[71] He also believes that political elites within purchasing governments, motivated by short term gains from spyware, are not deterred by the "outcasting" effect that typically serves to enforce international human rights.[72]

Enforcement issues notwithstanding, there is the question of whether *any circumstances* can legitimize a state's use of spyware technology under international law given the uniquely invasive nature of the tools. Dunja Mijatović, Commissioner for Human Rights of the Council of Europe, argues that it is "virtually unimaginable that the use of Pegasus or equivalent spyware could ever be considered in accordance with the law and the necessary safeguards as outlined by the [European Court of Human Rights]."[73] In other words, it is unclear if spyware could ever meet a proportionality test given that it provides operators with access to the entirety of one's life.[74] Other surveillance technologies, from wiretaps to stingrays[75], can be more easily restricted through judicial warrants. As Kaye notes, "it may be difficult, if not impossible, for a state to demonstrate its use of spyware for narrow purposes and without "collaterally" sweeping in personal data having no relevance to a legitimate governmental purpose."[76]

B. Export Control Laws Are Discretionary, Unreliable, and May Even Exacerbate Unlawful Spyware Use

States can also curtail potential human rights abuses associated with commercial spyware by limiting the technology's proliferation through blacklists or export control laws. Former UNHCR Michelle Bachelet advocated for states to not only take responsibility for their own use of spyware, discussed above, but also to limit the spread of

---

[71] Lubin, *supra* note 61, at 15.

[72] *Id.* at 15–16.

[73] FELDSTEIN & KOT, *supra* note 26, at 8.

[74] *See* Special Rapporteur, *supra* note 64, ¶ 24.

[75] A StingRay, or "cell site simulator" is a device that mimics a cell phone tower, forcing nearby cellular devices to connect to it. The technology is used by law enforcement to collect unique device identifiers—e.g., IMSI—and associate a target individual (via their device) with a geographic location. Stingrays are also used to collect the unique identifiers of all individuals present at a particular time and place—e.g., a protest or rally.

[76] David Kaye, *The Spyware State and the Prospects for Accountability*, 27 GLOBAL GOVERNANCE 1, 11 (2021).

these technologies: "Governments should immediately cease their own use of surveillance technologies in ways that violate human rights, and should take concrete actions to protect against such invasions of privacy by regulating the distribution, use and export of surveillance technology created by others."[77] Several years earlier, U.N. Special Rapporteur David Kaye made similar appeals for States to "condition export of such technologies on the strictest human rights due diligence."[78]

In July 2021, more than one hundred civil society organizations echoed the Commissioner's appeal, calling for a moratorium on the sale, transfer, and use of surveillance technologies.[79] "NSO Group and its competitors cannot regulate themselves, and governments should urgently suspend sales and transfers of surveillance technology while they investigate and regulate this industry," says Human Rights Watch advocate and researcher Deborah Brown. "Commercial spyware has been repeatedly used to target activists and journalists, and when left to their own devices, companies continue to sell these technologies to governments known to engage in abuses, including arbitrary surveillance, against perceived opponents."[80]

Many of these surveillance technology firms are based in Israel, which has effectively become the "Silicon Valley" of commercial spyware. Of the seventy-four governments that have procured commercial spyware and digital forensics technologies, fifty-six secured them from firms either based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru.[81] Israel's defense ministry is responsible for issuing export licenses for NSO Group's spyware, but the agency has failed to prioritize human rights considerations in its licensing.[82] Israel's lack of discretion in issuing export licenses for NSO Group's Pegasus reflects the insufficiency of export control law as a regulatory mechanism for spyware. Its defense ministry has stated that it approves the export of cyber products "exclusively to governmental entities, for lawful use, and

---

[77] Bachelet Statement, *supra* note 65.

[78] Special Rapporteur, *supra* note 64.

[79] *See* #Seguridaddigital et al., *Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale, Transfer and Use of Surveillance Technology*, AMNESTY INT'L (July 27, 2021), https://www.amnesty.org/en/documents/doc10/4516/2021/en/ [https://perma.cc/PGC7-VBX2].

[80] *Unchecked Spyware Industry*, *supra* note 43.

[81] FELDSTEIN & KOT, *supra* note 26, at 2.

[82] *See id.*

only for the purpose of preventing and investigating crime and counter terrorism . . . . In cases where exported items are used in violation of export licenses or end use certificates, appropriate measures are taken."[83] Whatever measures Israel may have taken, they have not prevented Pegasus from being used by governments that abused the tool.[84]

Despite its outsized impact on the spyware industry, Israel is not the only country with the power to influence NSO Group or the spyware market. Some argue that the United States and other democracies should use their economic and diplomatic power to pressure Israel to restrict commercial spyware exports to countries with poor human rights records. Unfortunately, the discretionary nature of export control makes it an unreliable method of safeguarding spyware from misuse. For example, despite the EU's strict export rules, member states can easily evade them through intentionally lax domestic implementation.[85] To wit, "companies commonly establish subsidiaries in member states that are willing to overlook spyware operations to evade EU controls."[86]

In November 2021, however, the U.S. placed NSO Group on a Commerce Department blacklist, preventing the company from receiving exports of U.S. hardware or software. Notably, only after the U.S. government used Pegasus on a trial basis and ultimately decided not to purchase the product did the Biden administration take the opportunity to trumpet its pro-democracy values, declaring that NSO Group's tools have "enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order."[87] The Commerce Department's listing has the power to cause significant economic damage to a firm like NSO Group, thereby helping to eradicate bad actors and incentivizing others to comply with international human rights standards. Being listed on the Entity List prevents NSO Group from

---

[83] Dan Williams, *Israel Says Spyware Exports Are For Lawful Use Only*, REUTERS (July 19, 2021, 6:28 PM), https://www.reuters.com/world/middle-east/liberals-israeli-govt-discuss-nso-spyware-with-defence-minister-2021-07-19/ [https://perma.cc/9BAY-LHRC].

[84] *See Unchecked Spyware Industry*, *supra* note 43.

[85] FELDSTEIN & KOT, *supra* note 26, at 14.

[86] *Id.*

[87] Press Release, U.S. Dep't of Com., Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/3WP3-UNE9].

accessing many technologies or products that originate in the U.S., such as critical computing equipment or software services, without special U.S. government approval. The listing can also make the company less attractive to investors. A researcher at Citizen Lab testified to the House Intelligence Committee in July 2022 that the debt valuation of NSO Group "precipitously dropped" following the Commerce Department's listing.[88]

That said, battling the spyware industry through export controls and sanctions is akin to fighting a multi-headed hydra. While export control laws can be highly effective in handicapping specific companies, they neither fully nor effectively regulate the industry. Given the growing demand for spyware technologies, putting one actor on a blacklist can incentivize buyers to go "down-market" to even less scrupulous companies that may emerge to fill the gap left by blacklisted companies,[89] thereby perpetuating underlying issues of accountability, transparency, and human rights. Even with Israel's leading spyware companies on the U.S.'s export control list, other less sophisticated firms sell similar products out of India, the Philippines, and Cyprus.[90] As top-tier commercial vendors like NSO Group face heightened public scrutiny or sanctions, a secondary tier of spyware purveyors may become more powerful.[91] In this context, it becomes easier for governments to hide their attacks in the "noise" of open source and commercially available malware.[92]

Sanctions and market regulations that force countries like Egypt or the UAE to purchase second tier—i.e., less powerful or effective—spyware from boutique operators arguably represent a positive outcome.[93] However, this qualified "win" for partially regulating the spyware market would still amount to an overall net loss for human rights given the number of firms that, as discussed, could find other ways to operate and meet demand.

---

[88] *Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware: Hearing Before the Permanent Select Comm. on Intelligence*, 117th Cong. 28 (2022) (statement of John Scott-Railton, Senior Researcher, Citizen Lab).

[89] FELDSTEIN & KOT, *supra* note 26, at 13 (explaining that Carnegie Institute's global inventory of spyware firms over the past decade shows newer market entrants like NSO Group, Cytrox, Candiru taking place of older suppliers like FinFisher and Hacking Team).

[90] *See* Deibert, *supra* note 2.

[91] *See* FELDSTEIN & KOT, *supra* note 26, at 2. Feldstein describes the composition of this secondary tier as "boutique spyware firms, hacker-by-night operations, exploit brokers, and similar groups." *Id.*

[92] *See* FELDSTEIN & KOT, *supra* note 26, at 11.

[93] *See id.* at 13.

C. Prospects for Voluntary Industry Self-Regulation Are Weak

Prior Parts discussed the role of states in preventing human rights abuses that stem from their use or distribution of spyware technology. However, under international law, what responsibilities do companies bear for applications of their technologies that violate international human rights standards? The United Nations Guiding Principles on Business and Human Rights (UNGPs) were established in 2011 to address this question through a soft law mechanism. It delineates the responsibilities of companies to (a) "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;" and (b) to "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products, or services by their business relations, even if they have not contributed to those impacts."[94] The UNGPs expect companies to voluntarily conduct human rights due diligence to regularly identify and address any human rights impacts associated with their past, present, and future business operations. Participating firms must have remediation processes for addressing any human rights violations that they have "caused" or to which they have "contributed."[95] In cases where "adverse impacts have occurred that the business enterprise has not caused or contributed to, but which are *directly linked* to its operations, products, or services by a business relationship," firms are not expected to provide remediation.[96] Rather, the company is expected to prevent or mitigate the impact.[97]

Technically, the lack of precise definitions for "causing," "contributing," and "direct linkage" under the UNGPs makes it more difficult to assess NSO Group's relationship to various human rights impacts and therefore, the expected or appropriate corporate response.[98] In practice, however, the difference between whether NSO Group's spyware product "contributed" or was "directly linked" to, say, a journalist's murder, is irrelevant if the company is responsible for serving as its own prosecutor, judge, and jury under

---

[94] UNGP, *supra* note 13.

[95] *Id.* ¶ 15.

[96] *Id.* ¶ 22 (commentary) (emphasis added).

[97] *See id.* ¶ 13.

[98] *See* Vivek Krishnamurthy, *With Great (Computing) Power Comes Great (Human Rights) Responsibility: Cloud Computing and Human Rights*, 7 BUS. AND HUM. RTS. J. 226, 241 (2022).

the UNGP regime. That is, compliance and enforcement mechanisms simply do not exist for the UNGPs.

NSO Group has tried to minimize any connection or link to the actions of its clients, seeking to absolve the company of responsibility for downstream human rights impacts. "[W]e do not have visibility into the specific operational uses of our products, unless that access is granted by the customer," says the company.[99] NSO Group has also stated that it "does not and cannot know who the targets of its customers are, yet implements measures to ensure that these systems are used solely for the authorized uses."[100]

Nevertheless, interviews conducted by the *New Yorker*'s Ronan Farrow suggest the opposite. "We hear about every, every phone call that is being hacked over the globe, we get a report immediately," said one former NSO Group employee.[101] "They can see everything that goes on," a senior European law enforcement official confirmed. "They have access to the database, they have access to all of the data."[102]

Despite the valuable standard-setting role that the UNGPs play for companies truly committed to social responsibility, the voluntary nature of the principles enables them to be co-opted by companies seeking to improve their reputation and public perception. One year after a well-publicized forensic analysis showed that Pegasus was linked to the murder of journalist Jamal Khashoggi, NSO Group's new investors, Novalpina Capital, announced a new governance plan for the company that claimed compliance with the UNGPs—even proclaiming that its human rights compliance goals would be the most ambitious within the cybersecurity industry.[103] NSO Group also references its commitment to the UNGPs in the opening sentence of its Human Rights Policy, saying that they "hold [themselves] to the

---

[99] TRANSPARENCY AND RESPONSIBILITY, *supra* note 19, at 10.

[100] Lily Hay Newman, *NSO Group Spyware Targeted Dozens of Reporters in El Salvador*, WIRED (Jan. 12, 2022), https://www.wired.com/story/nso-group-pegasus-el-salvador/ [https://perma.cc/T65G-3KG5].

[101] Farrow, *supra* note 22.

[102] *Id.*

[103] *See* Stephanie Kirchgaessner, *Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests*, THE GUARDIAN (July 18, 2021), https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus [https://perma.cc/2Z4W-QQBH]; Audrey Travère, *The Rise and Fall of NSO Group*, FORBIDDEN STORIES (July 19, 2021), https://forbiddenstories.org/the-rise-and-fall-of-nso-group/ [https://perma.cc/XZ34-DF6H].

highest standards for ethical business, taking all reasonable steps to prevent and mitigate the risk of misuse of [their] products."[104]

More pointedly, the company has repeatedly claimed that it does not tolerate misuse against "civil rights activists, journalists, or any innocent person."[105] If the company suspects misuse, a representative told the *New York Times* as early as 2018, "[NSO Group] investigate[s] it and take[s] the appropriate actions, including suspending or terminating a contract."[106] Indeed, in 2021, NSO Group reported that it terminated five contracts with clients who failed to meet international human rights standards and rejected more than $300 million in contracts for the same reason.[107]

These strongly worded internal human rights policies and safeguards appear to have limited effect. Only weeks after NSO's Transparency Report indicated that its contracts require customers "to use [NSO Group's] products solely for the prevention and investigation of serious crimes (including terrorism) and to ensure that the products will not be used to violate human rights,"[108] the Pegasus Project media consortium revealed the widespread targeting of more than 50,000 members of civil society via Pegasus spyware.[109] Given the large number of people targeted and the range of occupations targeted—not to mention the authoritarian regimes involved in the targeting—it is unlikely that all of these people were legitimately targeted under international law or were involved in serious crime or terrorism per NSO Group's intended use.[110]

The prospects for spyware industry self-regulation are weak. U.N. Special Rapporteur David Kaye warned of the inadequacy of self-regulation in the spyware industry in 2019: "Companies

---

[104] *Human Rights Policy*, NSO GROUP, https://www.nsogroup.com/governance/human-rights-policy/ [https://perma.cc/CY4U-LHY9].

[105] Azam Ahmed, *A Journalist Was Killed in Mexico. Then His Colleagues Were Hacked*, N.Y. TIMES (Nov. 27, 2018), https://www.nytimes.com/2018/11/27/world/americas/mexico-spyware-journalist.html [https://perma.cc/NSF5-5ZSU].

[106] *Id.*

[107] *See* Travère, *supra* note 103.

[108] TRANSPARENCY AND RESPONSIBILITY, *supra* note 19, at 17.

[109] Pegasus Project, *supra* note 3.

[110] States can restrict or interfere with human rights established under the ICCPR in order to protect national security, public safety, public order, or public health; however, any such interferences must be proscribed by law and "necessary in a democratic society." ICCPR art. 22, *supra* note 12. Therefore, under the ICCPR, a state cannot exceed what is necessary or legally proscribed and arbitrarily target individuals with spyware under a pretense of protecting national security.

appear to be operating without constraint. It is critical that companies themselves adhere to their human rights responsibilities, including by disclosing their transfers, conducting rigorous human rights impact assessments, and avoiding transfers to States unable to guarantee their compliance with their human rights obligations."[111] At present, the financial incentives for spyware firms to sell to any government interested in purchasing their products appear to outweigh their potential interest in conducting meaningful human rights due diligence in accordance with the UNGPs. The fact that NSO Group could easily claim that it had implemented policies in alignment with the UNGPs, only to then enable human rights abuses, is reflective of the manipulability and malleability of the UNGP regime.[112]

D. Multistakeholder Alternatives Are Unproven

Given the limitations of existing international human rights law, export control, and soft law, several scholars propose new multistakeholder approaches for regulating the commercial spyware industry. Asaf Lubin and Anna Chan each draw upon the international response to a comparable challenge: the rise of private military and security companies (PMCs) following the U.S. invasion of Afghanistan in 2001.[113] Despite major domestic reforms in the U.S. and other jurisdictions to hold PMCs accountable for their actions while under contract,[114] the global growth of a broadly unregulated PMC industry has led to significant human rights abuses, such as indiscriminate killings, property destruction, and sex trafficking.[115]

In the absence of any statutory means for holding private military and security contractors liable for illegal activities, the international

---

[111] Press Release, Off. Of the High Comm'r for Hum. Rts., UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools (June 25, 2019), https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance [https://perma.cc/CKU9-MSNU].

[112] *See* Lubin, *supra* note 61, at 25 n. 125.

[113] *Id.* at 6; Anna W. Chan, *The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware*, 44 BROOK. J. INT'L L. 795, 798 (2019).

[114] *See* Reema Shah, *Beating Blackwater: Using Domestic Legislation to Enforce the International Code of Conduct for Private Military Companies,* 123 YALE L.J. 2559, 2560–63 (2014).

[115] *See* EVGENI MOYAKINE, THE PRIVATIZED ART OF WAR: PRIVATE MILITARY AND SECURITY COMPANIES AND STATE RESPONSIBILITY FOR THEIR UNLAWFUL CONDUCT IN CONFLICT AREAS 10–32 (2015).

community developed the International Code of Conduct for Private Security Service Providers (ICoC)[116] and a related monitoring organization, the International Code of Conduct Association (ICoCA). Both the ICoC and the ICoCA were designed to increase PMCs' compliance with human rights norms and international humanitarian law.[117] By some measures, the ICoC and its oversight mechanisms represent a success. In addition to establishing norms for the PMC industry and its government clients, an impressive 708 companies signed the ICoC, and several key military states committed to making PMC contracts contingent upon membership in and compliance with the ICoC.[118] By other counts, the ICoC is a limited soft law mechanism which, lacking judicial bodies or punitive capabilities, is unable to demonstrably curtail or address human rights abuses. Ultimately, some scholars argue, the success of the ICoC depends upon the willingness of states to enact strong domestic legislation regulating their use of PMCs.[119]

Building upon the ICoC, Lubin proposes a "Commercial Spyware Accreditation System" (CSAS) that aims to regulate the commercial spyware industry through a legally binding international agreement among governments and companies.[120] Member states would only be allowed to procure spyware from vetted and approved CSAS vendors, and these companies would be obligated to adhere to discreet guidelines and oversight throughout the product lifecycle, from development to marketing to client termination.[121] Addressing an inadequacy of the ICoC model, participating countries would also be required to implement domestic policies governing the use of spyware in conformity with international human rights law.[122] That is, to lawfully deploy spyware under the CSAS, a state would need to prescribe its use through legislation, demonstrate necessity—e.g.,

---

[116] *See The International Code of Conduct for Private Security Service Providers*, INT'L CODE OF CONDUCT ASS'N, https://icoca.ch/the-code/ [https://perma.cc/E23U-B3WN].

[117] *See* Shah, *supra* note 114, at 2563–64.

[118] *See History*, INT'L CODE CONDUCT ASS'N, https://icoca.ch/en/history [https://web.archive.org/web/20201006035254/https://www.icoca.ch/en/history]; *see also The International Code of Conduct for Private Security Service Providers*, *supra* note 116, ¶18 ("Member and Affiliate Companies will make compliance with this Code an integral part of contractual agreements with Personnel and subcontractors or other parties carrying out Security Services under their contracts.").

[119] *See* Shah, *supra* note 114, at 2568.

[120] Lubin, *supra* note 61, at 42–49.

[121] *Id.* at 45–47.

[122] *Id.* at 43–44.

protecting national security, protecting rights of others—respect principles of proportionality, ensure adequate safeguards, and provide access to remedy.[123] Member states would also be required to assign national "contact points," individuals entrusted to oversee grievance mechanisms, including potentially facilitating conciliation or mediation.[124] Similar to the ICoCA's governance model, the CSAS would be governed by a board of directors comprised of government, corporate, and civil society representatives charged with reviewing spyware companies' membership applications and conducting annual oversight to ensure compliance.[125] The board would also address appeals in response to decisions made by national contact points as part of the grievance process.[126]

Chan proposes a similar (albeit less specific) "shared responsibility regime" comprised of both state and non-state actors cooperating to limit states' use of spyware, require procedural safeguards, and ensure access to remedy.[127] Chan's model requires states to not only monitor corporate actions to prevent human rights violations but also provide recourse to victims of human rights violations.[128]

In short, both Lubin and Chan advocate for regulatory regimes that facilitate compliance with international human rights laws and norms—i.e., ICCPR and UNGPs—by making it impossible for noncompliant spyware vendors to secure lucrative government contracts. The success of these proposals depends upon the significant engagement and participation of a critical mass of powerful states which, among other responsibilities, would be required to implement controversial domestic legislation regulating government uses of spyware and providing access to remedy. Limited state participation in the ICoC model, however, reveals the challenges of incentivizing participation in multistakeholder arrangements that constrain a state's access to military, intelligence, or security resources. To effectively regulate commercial spyware through a binding multistakeholder arrangement, successful proposals will need to overcome this challenge by finding ways to incentivize states to prioritize their commitment to safeguarding human rights over—or at least alongside—their demand for powerful intelligence technologies.

---

[123] *Id.* at 44–45.

[124] *Id.* at 43.

[125] *See id.*

[126] *See id.*

[127] Chan, *supra* note 113, at 799.

[128] *See id.*

III. UNIQUE OPPORTUNITIES FOR ACCOUNTABILITY THROUGH U.S. LITIGATION

As Part II established, international law does not offer a clear mechanism for holding non-state actors—i.e., corporations—accountable for breaching international human rights standards.[129] Thus, plaintiffs have more often turned to suing NSO Group in various domestic jurisdictions, including France, Spain, the U.K., and Israel.[130] Notwithstanding the potential for litigation in other countries, the U.S. functions as a unique jurisdiction given its role as home to the major technology firms that spyware companies depend upon for their exploits. Technology firms that are likely to be repeatedly impacted by spyware attacks are especially motivated to slow or stop the proliferation of businesses that prey on vulnerabilities in their hardware and software. "State-sponsored actors like the NSO Group spend millions of dollars on sophisticated surveillance technologies without effective accountability," decried Apple's senior vice president of software engineering, Craig Federighi, emphasizing that "[t]hat needs to change."[131] In some circumstances, the U.S. may also potentially serve as a jurisdiction for individual victims who may be unable to seek redress in other jurisdictions. This Part evaluates three pending court cases against NSO Group in U.S. federal courts and explores their introduction of a potential novel pathway for holding spyware companies accountable for the human rights violations stemming from the development and use of their products. After introducing complaints filed by WhatsApp, Apple, and the publication *El Faro*, respectively, I review the effectiveness of key arguments proposed by plaintiffs and the defendant, NSO Group.

---

[129] *See id.* at 806; *see also Developments in the Law: International Criminal Law*, 114 HARV. L. REV. 1943, 2025–26 (2001) ("[I]nternational law failed both to articulate the human rights obligations of corporations and to provide mechanisms for regulating corporate conduct in the field of human rights.").

[130] *See* Siena Anstis, *Litigation and Other Formal Complaints Related to Mercenary Spyware*, CITIZEN LAB (Dec. 12, 2018), https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ [https://perma.cc/DPW8-LF7V].

[131] Press Release, Apple, Apple Sues NSO Group Curb the Abuse of State-Sponsored Spyware (Nov. 23, 2021), https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/ [https://perma.cc/N7NB-6564] [hereinafter Apple Press Release].

A. WhatsApp v. NSO Group

In October 2019, WhatsApp and its parent company, Meta, became the first U.S. technology firm implicated in Pegasus attacks to file a claim against the foreign NSO Group. The complaint asserted that NSO Group had created multiple WhatsApp accounts and then "reverse-engineered" the WhatsApp software in violation of the terms of service to develop a program that could emulate WhatsApp network traffic.[132] This program had enabled NSO Group to send malicious code—undetected—to WhatsApp users via the company's servers.[133] The malware, which could be delivered through a missed call without any involvement from the victims, had triggered the download of Pegasus spyware onto targets' phones.[134] According to the complaint, "the spyware gave the attackers full access and control over victims' smartphones remotely, including access to messages that they normally could not access because of WhatsApp's end-to-end encryption as well as files, emails, call logs, text messages, photos, and videos—in short, everything."[135] The users targeted by the Pegasus attack had WhatsApp numbers with multiple country code prefixes, including those associated with the Kingdom of Bahrain, the United Arab Emirates, and Mexico, indicating the global reach of the attack.[136]

WhatsApp asserted four causes of action in its complaint filed in federal court in the Northern District of California. The company argued that the defendant, first, violated the CFAA[137] and second, several sections of the California Comprehensive Computer Data Access and Fraud Act[138] by accessing and using the plaintiff's servers without authorization and infecting 1,400 target users' devices with malware between April and May 2019.[139] Next, WhatsApp claimed that NSO Group violated the terms of service to which it had agreed, thereby breaching a contract under California law.[140] Finally, it asserted a trespass to chattels tort claim, arguing that NSO Group

---

[132] WhatsApp Complaint, *supra* note 15, ¶¶ 33, 35.

[133] *Id.* ¶ 35.

[134] *Id.*

[135] Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, 36 BERKELEY TECH. L. J. 469, 481 (2021).

[136] *See* WhatsApp Complaint, *supra* note 15, ¶ 43.

[137] 18 U.S.C. § 1030.

[138] *See* CAL. PENAL CODE § 502.

[139] WhatsApp Complaint, *supra* note 15, ¶¶ 58–66.

[140] *Id.* ¶¶ 67–73.

intentionally interfered with WhatsApp's computer systems, causing WhatsApp to incur losses and economic damage.[141]

In a July 2020 court order, the district court judge, taking the plaintiff's allegations as true, allowed the CFAA claims to proceed, but dismissed the tort claims, agreeing in part and denying in part NSO Group's motion to dismiss.[142] On the CFAA claims, the court confirmed that NSO Group had exceeded its authorized access to WhatsApp's servers, meeting the "breaking and entering" threshold set by prior courts.[143] The defendant argued that WhatsApp did not suffer any losses as defined by the CFAA because NSO Group had accessed individual users' devices—not WhatsApp's devices or servers.[144] However, the court validated WhatsApp's claims, affirming that "the Ninth Circuit has held that a plaintiff can recover for violation of the CFAA when a defendant accesses a third party's device as long as the plaintiff is harmed by such an act, particularly if the plaintiff has a right to data stored on the third-party device."[145]

The court dismissed WhatsApp's tort claims because the "complaint [had] not detail[ed] any actual harm caused by [NSO Group's] program or access to WhatsApp's computers or servers."[146] Under the Ninth Circuit precedent, *Intel Corp. v. Hamidi*,[147] the court reasoned that California law does not cover "an electronic communication that neither damages the recipient computer system nor impairs its functioning."[148] Resources expended to respond to the breach do not qualify as harm under *Hamidi* for the purpose of an electronic trespass to chattels claim.[149]

NSO Group attempted to have the charges dismissed primarily on jurisdictional grounds, not because the company denied its hacking activities.[150] Several of these questions will likely be relevant to how future claims against commercial spyware

---

[141] *Id.* ¶¶ 74–78.

[142] WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (July 16, 2020).

[143] *Id.* at 680 ("[N]o WhatsApp user had permission to access the technical call settings or evade WhatsApp's security and, thus, there was no authorization").

[144] *Id.* at 682.

[145] *Id.*

[146] *Id.* at 686.

[147] 71 P.3d 296 (Cal. 2003).

[148] *WhatsApp*, 472 F. Supp. 3d. at 684 (citing *Hamidi*, 71 P.3d 296 (Cal. 2003)).

[149] *See id.*

[150] Mot. to Dismiss, WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 19-07123 (N.D. Cal. Apr. 2, 2020).

companies are adjudicated. WhatsApp sought to establish jurisdiction in California on multiple grounds. First, it argued that NSO Group had targeted its actions to California and its residents, since WhatsApp—and its parent company, Meta—is incorporated and has its principal place of business in California.[151] Next, the computers that NSO Group allegedly breached were physically located in California.[152] Additionally, NSO Group, when creating WhatsApp accounts, had agreed to be bound by WhatsApp's terms of service, which names and compels California jurisdiction.[153] WhatsApp also claims that NSO Group availed itself of the state's resources by obtaining financing in California.[154] I address each jurisdictional claim by reviewing NSO Group's arguments for dismissal and the court's associated order.

First, NSO Group claimed that foreign governments—not NSO Group—had committed the alleged actions against WhatsApp.[155] According to the declaration of NSO Group's CEO and co-founder, the company's role is limited to "providing advice and technical support to assist customers in setting up—not operating—the Pegasus technology."[156] Therefore, it argued, the court not only lacked subject matter jurisdiction but as the agents of foreign sovereigns, NSO Group should also be entitled to foreign sovereign immunity and derivative sovereign immunity.[157] The district court held that NSO Group does not qualify as a foreign official acting in an official capacity.[158] As a private firm, it is also not entitled to the kind of derivative immunity that may sometimes apply to domestic contractors working for foreign sovereigns.[159] The Ninth Circuit

---

[151] *See* WhatsApp Complaint, *supra* note 15, ¶ 13 ("[T]hreatened and actual harm to WhatsApp and Facebook occurred in this District.").

[152] *Id.* ¶ 11.

[153] *Id.* ¶ 12.

[154] *Id.* ¶ 11.

[155] WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649, 669 (July 16, 2020).

[156] *Id*. at 670.

[157] *Id.* at 663 ("Defendants contend that the court lacks subject matter jurisdiction because the conduct giving rise to the complaint was performed by foreign sovereigns and the Foreign Sovereign Immunity Act ("FSIA") bars any lawsuit on that basis. Defendants also assert that the court should extend the doctrine of derivative sovereign immunity to them because defendants were contractors of the foreign sovereigns acting within the scope of their employment.") (citations omitted).

[158] *See id.* at 664–65.

[159] *See id*. at 666 (noting that the Ninth Circuit "has not held that the doctrine of derivative sovereign immunity applies to the foreign contractors

Court of Appeals affirmed the district court's decision, denying foreign sovereign immunity to NSO Group on November 8, 2021.[160]

Given that NSO Group's customers had been the ones who targeted California residents, NSO Group argued, WhatsApp had also failed to join parties. Citing a CFAA case against the State of Qatar alongside other plaintiffs,[161] in which the sovereign nation could essentially be excluded from the case without limiting the court's ability to provide relief to the plaintiffs, the court rejected the argument.[162] It reasoned that NSO's customers are not required parties because the court can craft injunctive relief that excludes or carves out any sovereign nation.[163]

The court's personal jurisdiction assessments are more nuanced. First, given how WhatsApp's terms of service were constructed, the court determined that NSO Group had not actually consented to California jurisdiction.[164] Therefore, the court declined to assert personal jurisdiction over the breach of contract.[165] Nevertheless, the court asserted personal jurisdiction for the case using pendant jurisdiction, which is applicable when "the breach of contract claim involves the same common nucleus of operative facts as the tort claims."[166] Applying the Calder jurisdictional test,[167] the court determined that NSO Group "retained some role in conducting the intentional act, even if it was at the direction of their customers."[168] Next, NSO Group's actions were aimed at California, the forum state, because it allegedly "caused a digital transmission to enter California, which then effectuated a breaking and entering of a server

---

of foreign sovereigns"). Compare this to the "domestic contractors" examples cited by NSO Group.

[160] *See* WhatsApp v. NSO Grp. Techs. Ltd., 17 F. 4th 930 (9th Cir. 2021).

[161] *See* Broidy Cap. Mgmt., LLC v. Qatar, No. 18-2421, 2018 WL 6074570 (C.D. Cal. Aug. 8, 2018).

[162] *See WhatsApp*, 472 F. Supp. 3d. at 679.

[163] *See id.* at 665.

[164] *See id.* at 669 ("The terms of service's forum selection clause do not apply to claims initiated by WhatsApp against its users and, therefore, defendants did not consent to personal jurisdiction.").

[165] *Id.*

[166] *Id.* at 678.

[167] *See id*. at 669 ("Under the Calder effects test, plaintiffs must show that defendants (1) committed an intentional act, (2) expressly aimed at the forum state, (3) caused harm that the defendant knew was likely to be suffered in the forum state.") (citing Calder v. Jones, 465 U.S. 783, 789–90 (1984)).

[168] *Id.* at 670.

in California."[169] Finally, the court determined that "if [NSO Group] did access [WhatsApp's] servers without authorization (or exceeded authorized access), then [it] would have known [it was] harming plaintiffs" in the forum state.[170]

In January 2023, the Supreme Court denied NSO Group's petition for certiorari.[171] The case is scheduled for trial on December 2, 2024.[172]

B. Apple v. NSO Group

Approximately two weeks after the Ninth Circuit's decision allowing *WhatsApp* to proceed to trial, Apple joined the fight against NSO Group. It filed its own suit in November 2021 based on the same series of attacks revealed by Citizen Lab and reported by the Pegasus Project.[173] The suit appears to be part of a larger proactive business strategy to defend the company's brand position as a leader in privacy and security. Alongside a news release trumpeting the court filing, Apple announced a $10 million contribution "to organizations pursuing cybersurveillance research and advocacy."[174] Like WhatsApp, Apple also claimed CFAA violations[175] and breach of contract, citing five violations of Apple's iCloud terms of service, which, among other things, specifically prohibit the transmission of "viruses or code intended to harm or interfere with normal operation of [Apple's] Service."[176] Apple also included claims of unjust enrichment and violations of the California Business and Professions Code,[177] neither of which are present in WhatsApp's complaint. As

---

[169] *Id.* at 672.

[170] *Id.* at 673.

[171] Order Den. Cert., WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 19-07123 (Jan. 9, 2023), ECF No. 162.

[172] Minute Entry, WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 19-07123 (Feb. 16, 2023), ECF No. 165.

[173] *See* Apple Complaint, *supra* note 16; *see also* MARCZAK ET AL, *supra* note 30; Pegasus Project, *supra* note 3.

[174] Apple Press Release, *supra* note 131.

[175] *See* Apple Complaint, *supra* note 16, ¶ 67 ("Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with the intent to defraud accessed the operating system on Apple's users' devices without authorization using information from Apple's servers and then installed highly invasive spyware on those Apple users' devices, and by means of such conduct furthered the intended fraud and obtained something of value.").

[176] *Id.* ¶¶ 62–79, 85–91.

[177] CAL. BUS. & PROF. CODE § 17200 (covering "any unlawful, unfair or fraudulent business act or practice.").

for unjust enrichment, Apple claimed that NSO Group had profited from the "data they wrongfully obtained from Apple's users' devices through the improper use of Apple's servers, which is the central component of their lucrative Pegasus spyware sold to customers and deployed against journalists, activists, and dissidents around the globe."[178]

Unlike the WhatsApp case, however, Apple did not attempt a tort claim. Apple's claims focused on NSO Group's breach of Apple software on users' devices. Per license agreements, Apple retains ownership over the software on users' devices. Whether motivated by legal strategy or reputation management, Apple's claims differed from those of WhatsApp in that they focused on the impacts to targeted users as opposed to vulnerabilities in the company's servers or central systems.[179] In fact, Apple went to great lengths to establish that the company's servers were not breached. In its press release, Apple explained the exploit as follows: "To deliver FORCEDENTRY to Apple devices, attackers created Apple IDs to send malicious data to a victim's device — allowing NSO Group or its clients to deliver and install Pegasus spyware without a victim's knowledge. Though misused to deliver FORCEDENTRY, Apple servers were not hacked or compromised in the attacks."[180]

Apple, like WhatsApp, claimed to have suffered harm and damage because NSO Group's actions had forced the company to devote resources to investigate and respond to the exploits, including developing security patches, upgrading software, and introducing new security measures. Apple also argued that Defendants' ongoing efforts to build malware that evades Apple's security systems forces technology firms into a costly, ongoing "arms race."[181]

NSO Group, in its motion to dismiss, asserted that Apple's complaint had failed to join parties and establish valid jurisdictional and CFAA claims.[182] First, NSO Group argued, none of Apple's computers or servers were violated, per their own admission; furthermore, NSO Group had not operated the Pegasus software it develops.[183] Therefore, NSO Group argued, any individual owners of Apple devices with claims against NSO Group's government

---

[178] Apple Complaint, *supra* note 16, ¶ 20.

[179] *Id.* ¶ 5 ("Defendants did not breach data contained on Apple's servers, but did abuse Apple services and servers to perpetrate attacks on Apple's users and data stored on users' devices.").

[180] Apple Press Release, *supra* note 131.

[181] Apple Complaint, *supra* note 16.

[182] *See* Mot. to Dismiss, Apple Inc. v. NSO Grp. Techs. Ltd., No. 21-09078, at *4, *8, *9 (N.D. Cal. Mar. 3, 2022).

[183] *See id.* at *13.

clients should have directed their claims to those governments and not to NSO Group.[184] Next, NSO Group argued that its alleged actions have no relationship to California and would be more appropriately addressed in Israeli court.[185] Finally, NSO Group attempted to dismiss Apple's CFAA claims by arguing that operating systems are not covered by the CFAA because the statute's language only addresses "computers."[186] Furthermore, NSO Group argued, Apple's alleged harms did not qualify as "damage or loss" as defined by the CFAA.[187]

The court has not yet ruled on NSO Group's motion to dismiss Apple's complaint, but it will likely draw upon the Ninth Circuit's recent jurisprudence from the *WhatsApp* case. As pointed out by the district court in *WhatsApp,* the Ninth Circuit has interpreted the CFAA to mean that parties other than a computer's owner—e.g., WhatsApp and Apple—can indeed be proximately harmed by violations of the statute.[188] The Ninth Circuit also affirmed that expenditures related to investigating and responding to unauthorized access of users' phones qualifies as a cognizable loss sufficient for stating a claim.[189] The *Apple* case was stayed in June 2022, pending the outcome of the NSO Group's petition to the Supreme Court.[190] The stay was lifted in February 2023 and the case remains active.[191] Apple seeks a permanent injunction, compensatory damages, and punitive damages.[192]

C. El Faro (Dada v. NSO Group)

A third major case was filed in December 2022 against NSO Group in the U.S. District Court for the Northern District of

---

[184] *See id.* at *1, ¶ 27.

[185] *See id.* at *4–*8 (discussing *forum non conviens*).

[186] *See id.* at *9, ¶ 17 ("The only 'protected computers' the complaint identifies are 'Apple's users' devices.' But Apple does not allege it owns those devices; rather Apple allegedly owns only the 'operating-system software' installed on them. Apple likewise does not, and cannot, allege that its operating-system software is a 'computer' under the CFAA.") (citations omitted).

[187] *See id.* at *9-*10.

[188] WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649, 682 (July 16, 2020).

[189] *See id.* at 683.

[190] Minute Entry, Apple v. NSO Grp. Techs. Ltd., No. 21-09078 (June 23, 2022), ECF No. 40.

[191] Minute Entry, Apple v. NSO Grp. Techs. Ltd., No. 21-09078 (Feb. 16, 2023), ECF No. 46.

[192] Apple Complaint, *supra* note 16, at 20–21.

California.[193] It marks the first case brought by individuals against the spyware manufacturer in the United States.[194] Unlike the prior two complaints, which feature technology firms as plaintiffs, lawyers at the Knight First Amendment Institute filed *Dada v. NSO Group* on behalf of fifteen employees of *El Faro*, an independent news organization in El Salvador which built a reputation for covering "corruption, violence, and human rights abuses" across Central America.[195] The goal of the lawsuit, according to *El Faro* director Carlos Dada, is to hamper the ability of spyware companies like NSO Group to operate with impunity and even generate revenue through the targeting of civil society.[196] "I'd like to believe that if more cases are opened in other parts of the world against these firms they would think twice before permitting their products to be used [to attack journalists]," says Dada.[197]

Much like the *WhatsApp* and *Apple* cases, the *Dada* complaint alleges violations of the CFAA as well as the related state statute, the California Comprehensive Computer Data Access and Fraud Act.[198] The fifteen *El Faro* staff named in the suit all alleged that their iPhones had been infected by Pegasus spyware and remotely monitored over a period of eighteen months, based on a joint investigation by Citizen Lab and Access Now.[199] The infections had affected a majority of the news organization's staff and coincided with the newsroom's investigation of corruption and abuses in the Salvadoran government.[200] Since this claim represents the first to be filed by individual spyware victims, several questions will need to be answered before it becomes a template for future claims levied by

---

[193] Dada Complaint, *supra* note 17.

[194] *See id.*

[195] Jameel Jaffer, *Why We're Suing NSO Group*, KNIGHT FIRST AMEND. INST. AT COLUMBIA UNIV. (Dec. 1, 2022), https://knightcolumbia.org/blog/why-were-suing-nso-group [https://perma.cc/286H-MW6B].

[196] *See* Julia Gavarrete, *15 Members of El Faro Sue NSO in US Federal Court for Pegasus Hacks*, EL FARO (Nov. 30, 2022), https://elfaro.net/en/202211/el_salvador/26559/15-Members-of-El-Faro-Sue-NSO-in-US-Federal-Court-for-Pegasus-Hacks.htm [https://perma.cc/Y3DJ-F2BK].

[197] *Id.*

[198] Dada Complaint, *supra* note 17.

[199] *See* Julia Gavarrete, Daniel Reyes & Óscar Martínez, *22 Members of El Faro Bugged with Spyware Pegasus*, EL FARO (Jan. 12, 2022), https://elfaro.net/en/202201/el_salvador/25936/22-Members-of-El-Faro-Bugged-with-Spyware-Pegasus.htm [https://perma.cc/XV6E-JFFN].

[200] *See id.*

individuals in the U.S. against NSO Group or others for similar spyware attacks.

First, can individual spyware victims effectively establish standing in federal court? The *Dada* plaintiffs will need to show that they suffered "concrete and particularized" injury.[201] The CFAA defines several types of allowable damage and loss for a valid claim.[202] The plaintiffs alleged several types of harm in their complaint in accordance with the statute: (a) diminished value of the mobile devices targeted due to their inability to be used as intended after learning that devices were compromised; (b) costs incurred investigating and remediating the attacks, including device replacement; and (c) mental anguish due to loss of privacy.[203] The *Dada* court is likely to find these harms to comport with the statutory definition.

Next, despite the strategic value of targeting an upstream player in spyware surveillance, is NSO Group the ideal defendant? NSO Group's previously unsuccessful argument in *WhatsApp* that Pegasus operators—i.e., the Salvadoran government— are the more appropriate parties to the claim may be more compelling in cases levied by individual victims rather than technology firms. The initial court order in *WhatsApp* suggests that NSO Group is a party to the claim by virtue of NSO Group's development of tools that specifically targeted WhatsApp's servers.[204] This claim is arguably less relevant in cases brought by individuals than in those brought by technology firms whose code or infrastructure serves as a conduit that needs to be infiltrated before targeting individuals. That said, it is likely easier to trace attacks back to a technology provider, NSO Group, than to a state operator. Even if individual plaintiffs could demonstrate that an attack came from a state authority, immunity laws, as referenced above, would protect the sovereign nation from liability.

Finally, how can individual plaintiffs establish jurisdiction, especially if many of them did not suffer harm within the U.S.? The *Dada* complaint argued that the court has personal jurisdiction because another court in the same jurisdiction had already exercised

---

[201] *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 555 (1992).

[202] 18 U.S.C. § 1030(e)(8)–(11) ("[T]he term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.").

[203] *See* Dada Complaint, *supra* note 17.

[204] *See* WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649, 671–73 (July 16, 2020).

personal jurisdiction in *WhatsApp*.[205] However, since the *Dada* court could easily find the facts of the case to be dissimilar to that of *WhatsApp*, the complaint also offers an alternative argument by suggesting that the Federal Rules of Civil Procedure provide for a federal court's personal jurisdiction over a claim that is not subject to any particular state's jurisdiction.[206] If establishing jurisdiction for a claim against a commercial spyware firm without a clear forum state is successful under this rule, it could open the door for other spyware victims to bring claims against foreign firms in U.S. courts.

In January 2023, the *Dada* case was assigned to the same judge who is presiding over *Apple v. NSO Group*, Judge James Donato.[207] This case will help answer some of the above questions and provide some indication of whether and how individual victims can bring successful claims against foreign spyware companies in U.S. courts.

D. Key Factors Impacting Viability of These and Other Future Spyware Cases

Now that NSO Group's foreign immunity claims have been rejected, the pending *WhatsApp* case has the potential to set a course for related federal civil cases, including the *Apple* and *Dada* cases discussed in this Note, as well as criminal cases. For example, if the court validates WhatsApp's CFAA claims, the FBI may decide to pursue a federal cause of action against NSO Group under the CFAA. Other U.S. companies implicated in spyware attacks may also attempt to hold foreign commercial spyware entities accountable, as evidenced by the *Apple* case. Indeed, several large technology firms made their interests known when the *WhatsApp* case moved to the federal appellate courts. In late 2020, Microsoft, Google, LinkedIn, Cisco, and several other companies filed an amicus brief in opposition to NSO Group's plea for immunity.[208] The former NSO Group CEO contends that these companies are simply concerned that Pegasus' growth challenges the technology platforms' power to influence, control, and even sell access to data managed by these firms.[209] "When governments use Pegasus," former NSO Group

---

[205] *See* Dada Complaint, *supra* note 17.

[206] *See* FED. R. CIV. P. 4(k)(2)

[207] *See* Dada Complaint, *supra* note 17; Minute Entry, Dada v. NSO Grp. Techs. Ltd., No. 22-07513 (Jan. 6, 2023), ECF No. 37.

[208] *See* Brief for Amici Curiae Microsoft Corp., Cisco Sys., Inc., GitHub, Inc., Google LLC, LinkedIn Corp., VMware, Inc., and Internet Ass'n in Support of Plaintiffs-Appellees, WhatsApp v. NSO, 472 F. Supp. 3d 649 (9th Cir. 2021) (No. 20-16408, 37) [hereinafter Brief for Amici Curiae].

[209] Farrow, *supra* note 22. The brief argued that extending foreign sovereign immunity to private, commercial spyware firms would not only

CEO Shalev Hulio says, "they're less likely to lean on platform holders for wider 'back door' access to users' data."[210]

Together, the three active cases discussed in this Note introduce several open questions for any spyware cases that may follow in U.S. courts. Based on the lessons learned to date from *WhatsApp*, *Apple*, and *Dada*, this Part identifies critical factors for establishing jurisdiction and making valid tort and CFAA claims against commercial spyware vendors.

1. Establishing Jurisdiction in the Era of Cloud Computing

The location of a plaintiff's server or device may open plaintiffs to jurisdictional issues or vulnerabilities in filing tort or CFAA claims. Both types of claims rely on the notion of physical trespass, or digital breaking and entering. If a company leases cloud servers, as is commonplace, then proving that a hacker intentionally directed its attacks at a *specific* server in a particular location, rather than incidentally, could prove challenging. The *WhatsApp* court order enabling the case to proceed turns in part on the fact that WhatsApp's signaling and relay servers, located in California, were specifically targeted by NSO Group. If the breach took place on the company's leased third-party servers, several of which happened to be in California but were also located elsewhere, however, it may have been more difficult to show that NSO Group specifically targeted servers in the forum state.[211] This presents a potential challenge for future cases in which a technology firm's distributed cloud infrastructure is targeted and the physical location is incidental or happenstance. Leasing third-party servers is common industry practice, so firms challenging spyware firms for hacking may need to find alternative ways to establish jurisdiction, including through a "network trespass theory," as discussed below.

2. Successful Tort and Contract Claims

---

contribute to the growth of the private cyber-surveillance industry worldwide but also serve to "place these tools in the hands of more governments, including governments likely to engage in riskier behaviors and at greater risk of losing control of such tools." Brief for Amici Curiae, *supra* note 208, at 9–10.

[210] Farrow, *supra* note 22.

[211] *See* WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649, 672 (July 16, 2020) ("Indeed, '[d]efendants contend the location of the server is fortuitous and their claims would have been the same if the servers were located in Cleveland, Paris, or Timbuktu.'").

Assuming other district courts apply *Hamidi*, as discussed above, successful electronic trespass to chattels tort claims will need to demonstrate actual harm *beyond* the financial costs of responding to a breach.[212] The *WhatsApp* court indicated that plaintiffs need to show direct *consequential* economic damage from a server trespass to make a valid tort claim, such as physical impairment of their computer systems.[213] This kind of damage is unlikely in spyware claims since, as the *WhatsApp* judge notes, the success of a spyware hack typically depends upon the ongoing functioning of the infiltrated service.[214] Finally, even though WhatsApp did not claim "loss of business reputation and customer goodwill," it could potentially represent cognizable harm under *Hamidi* for trespass to chattels in future spyware cases.[215]

Next, contract claims against a spyware firm for breaching terms of service may be insufficient for establishing an effective case. The *WhatsApp* court argued that if it were to accept the plaintiff's view, then "any user simply by accepting the terms of service and otherwise having no interaction with California could be said to have purposefully availed him or herself of California's laws."[216] Indeed, more than one legal scholar has criticized the *WhatsApp* case for relying too heavily on terms of service violations.[217] Successful cases challenging spyware vendors for their attacks are likely to have more success relying on code violations through the CFAA than tort or contract claims.

3. Successful CFAA Claims

The outcome of the *WhatsApp* case will have a significant impact on the applicability of the CFAA to other hacking-related spyware cases as well as the ability of U.S. companies to defend themselves and their users against commercial spyware attacks in the future. The

---

[212] *See id.* at 685 ("[D]istrict courts applying Hamidi and addressing similar financial injuries have found that a financial injury resulting from a trespass to a computer is not an actual harm actionable").

[213] *See id.*

[214] *Id.* at 684–85 ("In fact, defendants' program was reliant on WhatsApp's servers to function exactly as intended. Defendants' program is alleged to emulate legitimate WhatsApp network traffic in order to transmit malicious code, undetected, to a user's device over WhatsApp's servers.")

[215] *Id.* at 685 ("Plaintiffs are correct in pointing out that Hamidi did not explicitly foreclose a goodwill argument and the court considered such economic injuries as an alternative argument.").

[216] *Id.* at 675.

[217] Penney & Schneier, *supra* note 135, at 477.

CFAA was written in 1986, many years before the emergence of commercial spyware, let alone the modern Internet and associated encryption technologies. As such, legal scholars may differ on how the CFAA should be interpreted. Some legal analysts have critiqued the *WhatsApp* lawsuit for its application of the CFAA."[218]

Jonathon Penney and Bruce Schneier, however, make a forceful argument in defense of WhatsApp's CFAA claims by advancing a "network trespass theory of liability" that could be applied to *WhatsApp* as well as future cases.[219] A straightforward interpretation of the CFAA, they argue, would find that NSO Group accessed WhatsApp's users' devices without authorization, using the WhatsApp network as a *conduit* for sending malicious code to victims' smartphones that allowed NSO Group's clients unauthorized access.[220] Under this interpretation, WhatsApp was *not* hacked, and any other technology platforms whose networks serve as conduits for a spyware attack would similarly not be covered by the CFAA.

Penney and Schneier offer an interpretation of the CFAA underwritten by recent jurisprudence that WhatsApp could use to bolster its CFAA claims in the pending case. Their analysis is based on the understanding that WhatsApp provides and manages an encrypted messaging network. In this context, they argue that user devices should be treated as part of the same network – not as separate computer systems – for the purposes of determining CFAA liability.[221] This theory is based on the recent precedent-setting case, *Van Buren v. United States*,[222] which interpreted the CFAA's "unauthorized access" concept similarly to traditional trespass law: "The 'basic wrong' leading to criminal and civil liability under the CFAA is bypassing an access barrier—or 'gate'—in order to access, or go where you are not supposed to go, on a computer system or network."[223]

Applying the network trespass theory to *WhatsApp*, plaintiffs could argue that NSO Group was aware of code-based restrictions—

---

[218] *Id.* ("It has been derided as an exercise in public relations, and the lawsuit's CFAA claims criticized by various legal and cyber-security experts as 'muddled,' unclear, and 'odd.'").

[219] *Id.* at 478.

[220] *See id.*

[221] Penney & Schneier, *supra* note 135 at 110.

[222] Van Buren v. United States, 141 S. Ct. 1648 (2021).

[223] Penney & Schneier, *supra* note 135, at 472–73. Incidentally, this definition from *Van Buren* runs counter to NSO Group's assertion in *Apple*, where NSO Group argued that only computers, not software, are covered by the CFAA. *See* Mot. to Dismiss, *supra* note 182, at 17.

i.e., end-to-end encryption code—prohibiting it from accessing user communications within the WhatsApp network. It then violated that restriction by taking action to circumvent encryptions and access user communications and data. In this model, NSO Group's actions may qualify as trespassing on both users as well as the WhatsApp messaging network.[224] Despite the court's initial validation of WhatsApp's CFAA claims, the network trespass argument is arguably more promising and may serve as a more effective approach for future spyware claims that do not have the advantage of being able to show that a specific server was targeted in a particular forum state.

The willingness of courts to evaluate CFAA claims through the lens of network trespass theory could impact the ability of various technology firms to raise successful CFAA claims against commercial spyware firms like NSO Group. If courts interpret network trespass under the CFAA in ways consistent with *Van Buren*, then a hack targeting *any* user of an encrypted networking platform, from Facebook Messenger to Telegram, would constitute unauthorized access of the entire network, inviting claims from any U.S.-based technology company that owns the software. This focus on the trespass on a distributed network has the benefit of sidestepping jurisdictional issues associated with showing that a defendant targeted a *specific* server physically located in a specific jurisdiction, which can prove difficult, as outlined above. Applying network trespass theory, any U.S. technology firm, such as Apple, could then theoretically bring CFAA claims against a foreign commercial spyware firm for attacks on network users anywhere in the world.

CONCLUSION

Despite being the subject of repeated media exposés, U.N. reprimands, and U.S. blacklists, NSO Group does not appear to be in retreat. A recent Citizen Lab report indicates that NSO Group deployed three new "zero-click" exploits in 2022 to penetrate the most current versions of Apple's software.[225] The question of how to effectively prevent Pegasus and other spyware tools from proliferating and violating human rights remains open. This Note argues that litigation in U.S. courts offers a unique and promising new avenue.

---

[224] *See* Penney & Schneier, *supra* note 135, at 486.

[225] *See* Joseph Menn, *They Were Investigating a Mass Kidnapping. Then Their iPhones Were Hacked.*, WASH. POST (Apr. 19, 2023), https://www.washingtonpost.com/technology/2023/04/18/nso-apple-iphones-citizen-lab/ [https://perma.cc/2YQ9-VCPL].

First, this Note reviewed the dynamics influencing a growing worldwide spyware marketplace and the types of harm that these tools can cause, both to democracies (chilling effects on speech and association, violations of privacy rights) and to individuals (from mental and physical harm to death). Next, this Note surfaced the major limitations of existing international regimes— human rights law, export control law, and soft law—in holding commercial spyware companies accountable for human rights violations associated with the use of their products. A human-rights-compliant regulatory framework does not presently exist for the sale, transfer, and use of surveillance technologies. A multi-stakeholder solution like the proposed CSAS is compelling but at present, merely aspirational.

Finally, this Note reviewed the three complaints filed against NSO Group in U.S federal courts as a means of assessing the potential for companies and individuals to hold NSO Group accountable for its customers' hacking activities. The *WhatsApp* court order provides useful guidance to Apple and other plaintiffs seeking to advance claims against NSO Group. The discussion reveals that spyware-related claims under the CFAA may have a higher likelihood of success than tort and contract claims, especially if courts adopt the network trespass theory of liability.

While U.S. litigation does not obviate the urgent need for global accountability and regulatory regimes that can forcefully govern spyware in accordance with international human rights law, U.S. courts can make a unique and important contribution to closing the regulatory gaps for the burgeoning commercial spyware industry in the interim.